Ph.D. Title Proposal

on

Intelligent Forensic Model for Network Attacks on Smart Devices

Submitted in partial fulfillment of the requirement
for the award of the Degree of

Doctor of Philosophy
in
Computer Applications

by

Milind D. Meshram

under the guidance of

Dr. Suhasini Vijaykumar

Computer Applications
Bharati Vidyapeeth's
Institute of Management and Information Technology
CBD Belapur, Navi Mumbai -400614
University of Mumbai
February 2023

Faculty: Technology(Computer Applications)

Area: Cyber Forensic

Topic of Thesis: Intelligent Forensic Model for Network Attacks on Smart Devices

Date of Admission: 26/08/2021

Name of Research Centre: Bharati Vidyapeeth's Institute of Management Information Technology, CBD Belpaur Navi Mumbai 400614

Name of Student: Milind D. Meshram

Name of Supervisor: Dr. Suhasini Vijaykumar

Signature of Student

Signature of Supervisor

Date of Submission
12/12/2022

Signature of Dean R&D

Signature of Principal

Name of Guide

Dr. Suhasini Vijaykumar
PRINCIPAL
Bharati Vidyapeeth's
Institute of Management & Information Technology
Sector-8, C.B.D. Belapur,
Navi Mumbai- 400 614.

NAVI MUMBAI

Index

Sr. No	**Contents**
	Abstract
01	Rational and Significance of Study
02	Issues and Challenges
03	A Survey of Work Done in the Research
04	Gap in the Literature Survey
05	Motivation
06	Statement of Aims and Objectives
07	Methodologies and Techniques to be used
08	Plan of Research
09	Outcome Expected
	References

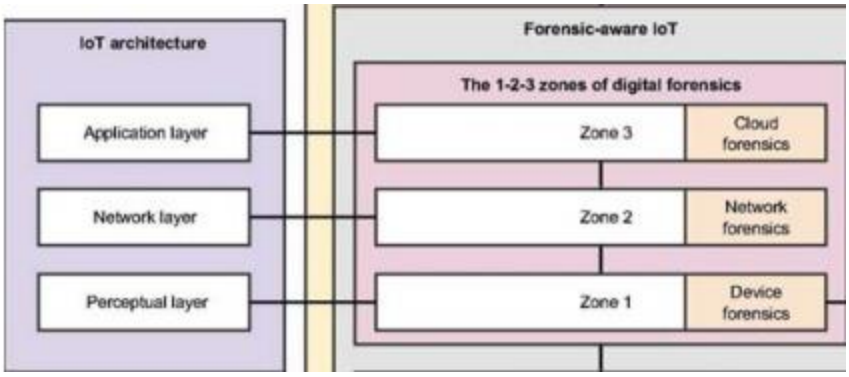
Abstract:-

The Internet of Things (IoT) has brought virtually unlimited possibilities for the development of smart applications that target everyday life improvement. Smart devices are often connected to the internet so they are vulnerable to a wide range of network attacks. Network Forensics is a scientific process to find out malicious traffic from the incoming/outgoing network traffic information. The investigator needs to follow correct investigative procedures so that the evidence recovered during the investigation will be authentic and accurate. Network forensic tools are used as collectors, analyzers, and visualizers that can assist investigators with network forensics but these tools cannot extract meaning from the packet of logs so intelligent technique using machine learning is required. Most of the smart devices' forensic frameworks are either conceptual or only focus on certain phases of the forensic process.

The outcome of this systematic literature review-based discussion discloses the dimensions of ongoing challenges in implementing help the development of an intelligent forensic model for network attacks on smart devices.

1. Rationale and Significance of Study

Smart devices such as smartphones, tablets, and smart home devices have less computational power, storage space, and memory size. By the year 2025, there may be 27 billion smart devices online, as per the IoT market forecast [33]. Smart devices are often connected to the internet so they are vulnerable to a wide range of network attacks, including botnet, malware, phishing, and denial of service attacks.



Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting electronic evidence.

Network Forensics is a scientific process to find out malicious traffic from the incoming/outgoing network traffic information.

Smart devices are more vulnerable due to their diversity. Forensics of smart devices research is in its early stage. There are many Challenges in the forensic Investigation of the smart device due to the Diversity of devices/protocols and Distributed data. Past studies primarily focus on the acquisition of data from devices/networks or attack detection and classification.

The investigator needs to follow correct investigative procedures so that the evidence recovered during the investigation will be authentic and accurate. Network forensic tools are used as collectors, analyzers, and visualizers that can assist investigators with network forensics but these tools cannot extract meaning from the packet of logs so intelligent technique using machine learning is required.

An intelligent forensic model can identify and analyze those attacks which will help to develop a strategy for preventing and mitigating those attacks.

Significance of study:

As more and more devices are connecting to the internet, resulting in the continued rise of cyber attacks so defense against these attacks is important for the individual as well organization.

2. Issues and challenges

Smart devices have less computational power, storage space, and memory size[1].Smart devices are electronic devices that can connect to the internet and be controlled remotely, typically through a smartphone or other mobile device. Examples of smart devices include smart thermostats, smart speakers, smart TVs, and smart home security systems. These devices can be used to automate various tasks, such as adjusting the temperature in a room or turning on the lights, and can also provide information and entertainment [2]. Security of the IoT environment is one of the challenges [3] due to the diversity of IoT devices.

Forensic investigators acquire and analyze data using traditional digital forensic methods[4]. IoT systems have varying functions, customized operating systems/file structures, and several wireless transmission protocols. This makes it difficult to identify and acquire data from IoT devices. Lack of Technical Capability Garfinkel [5] identified that many tools and techniques that once worked with traditional forensics would become obsolete due to the progress of technology. Evidence is usually short-lived as packets are produced from a single machine and sent through intermediate nodes to their destination so they need to capture and store in the form of logs[6].

3. A Survey of Work Done in the Research Area

Chung et al.[7] proposed a forensic framework CIFT(Cloud-based IoT Forensic Tool Kit) to identify, collect and analyze forensic data from the cloud as well as local devices for the Amazon Alexa ecosystem. However, this solution is limited to the Amazon Alexa ecosystem.

Kebande and Ray [30] proposed a generic digital forensic investigation framework for the internet of things DFIF-IoT which compiles with the ISO/IEC 27043: 2015 international standard for effective digital crime investigation of IoT infrastructure. Framework provides three modules: 1. Proactive process for forensic readiness 2. IoT forensic (Cloud Forensic, Network Forensic, and Device level Forensic), and 3. A reactive process occurs after the incident. It's a conceptual framework.

Babun et al. [18] proposed a digital forensic framework for smart environment IoTDots presents a comprehensive solution that automatically collects/stores forensically-relevant data from a

smart environment considering the interaction between users, devices, and apps inside the smart environment and the security policies defined for every different environment. It depends on the data privacy principle and not on Devices with limited resources

Zawoad and Hasan [9] proposed FAIoT, a forensic-aware ecosystem for IoT to collect forensic data from IoT platforms. It has a Secure Evidence Preservation Module to monitor all registered IoT devices and preserve the confidentiality of data. Secure Provenance Module for the secure chain of custody. IoT presents a general platform to collect forensic data systematically and organizes data for further analysis. But no implementation of data analysis.

Meffert et al.[11] has proposed FSAIoT a framework for IoT device state acquisition for the main focus on digital forensics on IoT devices which uses a controller for the state (On/Off) acquisition from IoT devices. it is not a forensically sound method IoT Network device fingerprinting will be future work.

Fagbola and Hein [31] proposed smart digital forensic readiness of organizations with shadow IoT devices. Shadow IoT devices are smart devices connected to a network without the knowledge of a network administrator. Framework has six steps including IoT device identification, monitoring, and evidence capture and preservation for forensic readiness so that organizations and individuals should be ready for digital forensic investigation.

Zhang[10] has done a detailed forensic case study of the Mirai botnet server by Practically Setting a fully functioning Mirai botnet network architecture and conducting a comprehensive forensic analysis on the Mirai botnet server remotely and by physical access to getting an IP address and user credential of the victim from Mirai Server. This forensic investigation is limited to the attacker's machine, not the victim's machine.

Amarantidou [15] suggested to use network forensic tools such as tcpdump, Wireshark (Ethereal), NetworkMiner, NetWitness Investigator, Kismet, Ngrep, EtherApe, and Snort (signature/rules-based IDS) as these tools are used as collectors, analyzers, and visualizers that

can assist investigators with network forensics but these tools cannot extract meaning from the packet of logs [25], [16-21]

Patil, R. Y [22] observed that attackers can spoof the IP address so source IP address information in the IP header of the packet cannot consider evidence against an attacker; existing techniques can reach up to the first edge router of the attacker. Most of the network forensic tools do not reach beyond ISP which is a very big challenge.

Zhang et al. [23] proposed a device identification technique based on real-time traffic feature extraction and fingerprint construction is proposed. The information from the TCP/UDP network data flows is mapped to the type of IoT device but it has an issue it depends on traffic and open port and it uses a machine learning approach to generate device fingerprint and is not forensically sound as it used dynamic features.

Hossain [12] has proposed a blockchain-based procedure for the credibility and authenticity of logs produced by IoT devices. But this approach takes a lot of processing power and time and every IoT device is not capable of it.

Cebe [13] proposed Block4Forensic an Integrated Lightweight blockchain framework for forensic application of connected Vehicles. This blockchain infrastructure provides storage of hashed data in the shared ledger and details (non-hash data) stored in the fragmented ledger.

Patil R. Y [14] proposed a methodology to uniquely identify devices used for cybercrime. The author proposed a hash tree-based tamperproof device fingerprint that uses hardware-based parameters like motherboard, CPU, BIOS, NIC, Disk Drive, and Timestamp information. which satisfied all the evidence characteristics mentioned in Indian Evidence Act., IoT compatibility was not verified.

Alizadeh [26] proposed public blockchain and InterPlanetary File System (IPFS) distributed hash table (DHT) technology to store information immutable and decentralized manner and to solve the storage and time problem of blockchain technology. DHT uses hash tables where key-

value pairs are stored, hash tables are more efficient than search trees, so hash table-based device fingerprints will be more efficient than hash tree-based device fingerprints.

Alsulami [27] proposed an automated and intelligent intrusion detection system using machine learning to detect and classify network activity on an IoT system. It has used a machine-learning classifier SNN, DT, BT, SVM, and KNN to classify normal, Mirai attacks, DoS attacks, Scan attacks, and MITM attacks. SNN, DT, and BT give 100% accuracy while KNN gives 99.80% and SVM gives 99.40% accuracy.

Dutta et al. [28] addressed an ensemble approach incorporating deep learning algorithms for an effective anomaly-based network intrusion detection system. Train and tested on IoT-23, LITNET-2020, and NetML-2020 datasets to assess the effectiveness. The author combines DNN and LSTM to increase accuracy but suggested to use of Big data like Apache spark to further improve the performance.

HaddadPajouh et al. [29] have proposed a recurrent neural network-based approach(LSTM) for IoT malware threat hunting and achieved a detection accuracy of 98.18 % against the IoT malware. Suggested that the Explainability of LSTM models proposes a more transparent DL model for detecting IoT cyber attacks, particularly those in an adversarial setting.

Koroniotis et al. [34] proposed a network forensic framework, named Particle Deep Framework (PDF), based on particle swarm optimization and deep learning for tracing attack origins and detecting them in IoT networks and capable of distinguishing between normal and attack traffic with an accuracy of about 99.9%. Train and tested the BoT-IoT dataset which covers three types of attacks covered ie Probing attacks, DDOS attacks(DOS and DDOS), and Identity theft attacks (data theft and keylogging).

Ref	*Attacks*	*Dataset*	*Methodology*	*Limitation*
Hassan et al. [34]	Exploits ,DoS Backdoor, Analysis, Fuzzers ,Generic Reconnaissance, Shellcode ,Worms	UNSW-NB15, ISCX2012.	CNN-WDLSTM	*Non IoT dataset*
Hassan et al. [35]	*BotNet*	*N-BaIoT 2018*	*DNN-LSTM*	*Only classify as Benign, Mirai, Gafgyt*
Alzahrani & Bamhdi, [36]	Mirai and BASHLITE.	N-BaIoT	*CNN-LSTM*	*NA*
Toupas et al. [37]		CICIDS2017	Synthetic Minority Over-Sampling Technique (SMOTE)	*Non IoT dataset*
Zhang et al. [38]	10 different types of attack	CICIDS2017 dataset and the CTU dataset	*CNN-LSTM*	*Non IoT dataset*
Cvitić et al [39]	DDoS UDP,TCP,IMPS	Generated dataset	Logical model tree	*NA*
Aakash et al.[40]	BotNet	Aposemat IoT-23 Dataset , N-BaIoT Dataset	Random Forest with Independent Component Analysis (ICA)8	*NA*
Prabhu & Nethravathi[41]	Cyber attack	*UNSW-NB 15*	Bi- Relu – ResNet	*Non IoT dataset*
Bhuvaneswari et al[42]	IoT attacks	NSL KDD, UNSW NB, CICIDS, CSE-CIC-IDS, and UNSW Bot-IoT.	A Layered Paddy Crop Optimization-Based Capsule Network	*NA*
Wang et al. [43]	Network attacks	UNSW-NB15	SSAE-BiGRU-Att model	*NA*

From Literature survey it has been observed that Most of researcher has used hybrid model using CNN LSTM. Capsule network and dynamic routine technique used to overcome drawback of Convolutional Neural Network which required lots of training data and Bi-GRU has the shortest training time and testing time while maintaining high classification accuracy, Bi-GRU + Capsule network to detect attack has not been studied yet.

4. Gap in the Literature Survey

- Most of the smart devices forensic frameworks are either conceptual or only focus on certain phases of the forensic process.
- Current network forensic tools can assist investigators, but there is a need for intelligent techniques to be implemented.
- Most of the IoT attack detection machine learning techniques are trained on legacy datasets such as KDD99 and NSL-KDD 99 datasets which are not truly IoT datasets except the Shivanathan dataset and BoT- IoT dataset.
- Earlier detection of attacks before a botnet attack is not commonly considered.
- Bi-GRU + Capsule network to detect attacks has not been studied yet.

5. Motivation

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting electronic evidence.

Smart devices are more vulnerable due to their diversity. Forensics of smart devices research is in its early stage. There are many Challenges in the forensic Investigation of the smart device due to the Diversity of devices/protocols and Distributed data.

Past studies primarily focuses on the acquisition of data from devices/network or attack detection and classification.

Widely used network forensic tools can only assist investigators but cannot exact meaning from packets and logs.

6. Statement of Aims and Objectives

To propose and design Intelligent Forensic Model for Network Attacks on Smart Devices.

Proposed research has following objectives.

- To study existing forensic models for detecting network attacks on smart devices.
- To design a forensic model for detecting network attacks on Smart Devices.
- To develop an algorithm to detect network attacks on Smart Devices using machine learning.
- To compare the proposed model with the existing model/tools based on various parameters.

7. Methodology and Techniques to be used

A systematic literature survey is carried out on several facets of the proposed research topic, in various peer-reviewed journals, patents, books and other research resources. This would be followed by the development of proposed model and compare it with the existing model,

- To Study existing model and identifies the challenges in them, study solutions available so far, and identify the parameters that contribute most to the forensic model of smart devices.
- Gather the network attack datasets of different types of attack and apply feature selection and feature selection network attack.
- To design testbed /simulation to test proposed model.
- Develop the model based on selected features.
- Train the model on the training dataset to classify the attack.

8. Plan of Research

	First Year				Second Year				Third Year			
	Quarters				Quarters				Quarters			
	1	2	3	4	1	2	3	4	1	2	3	4
Identify Research Area	■											
Formulate research questions		■										
Formulate research strategy, research design and select methods			■									
Define research question			■									
Research proposal				■								
Literature review				■								
Monitor literature and add to review					■							
Publication						■	■	■				
Data set Analysis									■			
Design and Implementation										■		
Simulation											■	
Analysis											■	
Publication									■	■		
Dissertation due												■

9. Expected Outcome

- Study existing forensic models for network attacks on smart devices.
- Design a forensic model for detecting network attacks on Smart Devices.
- Detect network attacks on Smart Devices using machine learning.
- Compare the proposed model with the existing model based on various parameters.

10. References

1 . King, J., & Awad, A. I. (2016). A distributed security mechanism for resource-constrained IoT devices. *Informatica*, *40*(1)

2. Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, *18*(3), 817

3. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal*, *5*(4), 2483-2495

4. Wu, T., Breitinger, F., & Baggili, I. (2019, August). IoT ignorance is digital forensics research bliss: a survey to understand IoT forensics definitions, challenges, and future research directions. In *Proceedings of the 14th International Conference on Availability, Reliability, and Security* (pp. 1-15)

5. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *digital investigation*, *7*, S64-S73

6. Ansari, A. Q., & Khan, M. A. (2012). A Journey from Computer Networks to Networks-on-Chip. *IEEE Beacon*, *31*(1), 71-77

7. Chung, H., Park, J., & Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital investigation*, *22*,S15-S25

8. Babun, L., Sikder, A. K., Acar, A., & Uluagac, A. S. (2018). Iotdots: A digital forensics framework for smart environments. *arXiv preprint arXiv:1809.00745*

9. Zawoad, S., & Hasan, R. (2015, June). Faiot: Towards building a forensics aware eco system for the internet of things. In *2015 IEEE International Conference on Services Computing* (pp. 279-284). IEEE

10. Zhang, X.,Upton, O., Beebe, N. L., & Choo, K. K. R. (2020). IoT botnet forensics: A comprehensive digital forensic case study on Mirai botnet servers. *Forensic Science International: Digital Investigation*, *32*, 300926

11**.** Meffert, C., Clark, D., Baggili, I., & Breitinger, F. (2017, August). Forensic State Acquisition from Internet of Things (FSAIoT) A general framework and practical approach for IoT forensics through IoT device state acquisition. In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (pp. 1-11)

12. Hossain, M., Karim, Y., & Hasan, R. (2018, July). FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. In *2018 IEEE International Congress on Internet of Things (ICIOT)* (pp. 33-40). IEEE

13 .Cebe, M., Erdin, E., Akkaya, K., Aksu, H., & Uluagac, S. (2018). Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE communications magazine*, *56*(10), 50-57

14. Patil, R. Y., & Devane, S. R. (2020). Hash tree-based device fingerprinting technique for network forensic investigation. In *Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2019* (pp. 201-209). Springer Singapore

15. Amarantidou, P. (2018). Computer and Network Forensics: investigating network traffic

16, NIKSUN (2013) 'NetDetectorLive' [Online] *https://www.niksun.com/c/1/ds/NIKSUNDatasheet_NetDetectorLive.pdf*

17. NIKSUN (2023) 'NetDetector' [Online] *https://www.niksun.com/c/1/ds/NIKSUNDatasheet_NetDetector.pdf*

18. Xplico (2013) 'Xplico Features' [Online] *http://www.xplico.org/about*

19. DeepNines Security edge Platform. (2008) "Deepnines Active Directory User Services Guide" Version 1.0

20. Brief, R.S. (2008). "The RSA enVision Platform A Single, Integrated 3-in-1 Log Management Solution." [online] https://www.indevis.de/sites/default/files/downloads/2017-06/RSA_envision_platform.pdf

21. Wireshark [Online] https://www.wireshark.org/docs/wsug_html/

22. Patil, R. Y., & Devane, S. R. (2019). Network forensic investigation protocol to identify true origin of cyber crime. *Journal of King Saud University-Computer and Information Sciences*.

23. Zhang, Y., Gong, B., & Wang, Q. (2022). BLS-identification: A device fingerprint classification mechanism based on broad learning for internet of things. *Digital Communications and Networks*.

24. Ahmad, L., Khanji, S., Iqbal, F., & Kamoun, F. (2020, August). Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In *Proceedings of the 15th international conference on availability, reliability and security* (pp. 1-8)

25. Easttom, C. (2021). *A systematic framework for network forensics based on graph theory* (Doctoral dissertation, University of Portsmouth)

26. Alizadeh, M., Andersson, K., & Schelén, O. (2020, December). Efficient decentralized data storage based on public blockchain and IPFS. In *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)* (pp. 1-8). IEEE

27. Alsulami, A. A., Al-Haija, Q. A., & Tayeb, A. (2022). Anomaly-based Intrusion Detection System for IoT Networks With Improved Data Engineering.

28. Dutta, V., Choraś, M., Pawlicki, M., & Kozik, R. (2020). A deep learning ensemble for network anomaly and cyber-attack detection. *Sensors*, *20*(16), 4583

29. HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A deep recurrent neural network based approach for internet of things malware threat hunting. *Future Generation Computer Systems*, *85*, 88-96

30. Kebande, V. R., & Ray, I. (2016, August). A generic digital forensic investigation framework for internet of things (iot). In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 356-362). IEEE

31. Fagbola, F. I., & Venter, H. S. (2022). Smart digital forensic readiness model for shadow IoT devices. *Applied Sciences*, *12*(2), 730

32. Koroniotis, N., Moustafa, N., & Sitnikova, E. (2020). A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. *Future Generation Computer Systems*, *110*, 91-106

33. IoT Market forecast [online] https://www.iotforall.com/state-of-iot-2022 09/02/2023

34. Hassan, M. M., Gumaei, A., Alsanad, A., Alrubaian, M., & Fortino, G. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences*, *513*, 386-396

35. Hasan, T., Malik, J., Bibi, I., Khan, W. U., Al-Wesabi, F. N., Dev, K., & Huang, G. (2022). Securing industrial internet of things against botnet attacks using hybrid deep learning approach. *IEEE Transactions on Network Science and Engineering*

36. Alzahrani, M. Y., & Bamhdi, A. M. (2022). Hybrid deep-learning model to detect botnet attacks over internet of things environments. *Soft Computing*, *26*(16), 7721-7735

37. Toupas, P., Chamou, D., Giannoutakis, K. M., Drosou, A., & Tzovaras, D. (2019, December). An intrusion detection system for multi-class classification based on deep neural networks. In *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)* (pp. 1253-1258). IEEE

38. Zhang, Y., Chen, X., Jin, L., Wang, X., & Guo, D. (2019). Network intrusion detection: Based on deep hierarchical network and original flow data. *IEEE Access*, *7*, 37004-37016.

39. Cvitić, I., Perakovic, D., Gupta, B. B., & Choo, K. K. R. (2021). Boosting-based DDoS detection in internet of things systems. *IEEE Internet of Things Journal*, *9*(3), 2109-2123

40. Akash, N. S., Rouf, S., Jahan, S., Chowdhury, A., & Uddin, J. (2022). Botnet Detection in IoT Devices Using Random Forest Classifier with Independent Component Analysis. *Journal of Information and Communication Technology*, *21*(2), 201-232

42. Prabhu, S., & Nethravathi, P. S. (2022). A Novel Approach of BRELU RESNET Based Cyber Attack Detection System with BAIT Based Approach for Mitigation. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *6*(1), 243-258

43. Wang, J., Chen, N., Yu, J., Jin, Y., & Li, Y. (2020, November). An efficient intrusion detection model combined bidirectional gated recurrent units with attention mechanism. In *2020 7th International Conference on Behavioural and Social Computing (BESC)* (pp. 1-6). IEEE